SUPPLEMENTAL RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**323-8281**
SRP Section:	**07.03 – Engineered Safety Features Systems**
Application Section:	**07.03**
Date of RAI Issue:	**11/30/2015**

Question No. 07.03-7

Describe how the voting logic for both reactor trip and engineered safety features systems in the APR1400 design will be automatically changed when one channel identifies a single failure and a second channel is in maintenance bypass. Also describe where the maintenance bypass mode will be set and reset for a channel.

10 CFR 50.55a(h)(3) states “Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under Part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603–1991 and the correction sheet dated January 30, 1995.” IEEE Std. 603-1991, Clause 6.7 requires, in part, that capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of Clauses 5.1 and 6.3.

APR1400 FSAR Tier 2, Sections 7.2 and 7.3, and Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System,” identify two-out-of-four coincidence logic for safety I&C systems would be changed to a two-out-of-three control logic if one channel is tripped. However, there is lack of design information describing how the coincidence voting logic will be modified to meet the above regulatory requirements for both reactor trip and engineered safety features systems in the APR1400 design when one channel is in a maintenance mode and at the same time another channel is tripped. Also it is not clear in the application where the bypass mode will be set and reset for a channel. Describe how the voting logic would be altered for all reactor trip and ESF functions for cases of single failure, maintenance bypass, and both simultaneously. In addition, provide design information on where the maintenance bypass mode will be set and reset for a channel.

Response

[Response to ‘Describe how the voting logic would be altered for reactor trip and ESF functions for a single failure of one channel’]

Section 3.4.4 of the Safety I&C System technical report states that the prevention of a spurious trip due to a single failure is assured by 2-out-of-3 voting logic in conjunction with a channel bypass function.
Also, Section 7.2.2.1 of DCD Tier 2 states the 2-out-of-4 voting logic prevents a system-level spurious actuation due to any single failure.

In conclusion, a channel bypass is applied to the channel where a single failure has occurred to avoid spurious reactor trip and ESF initiation due to that channel, resulting in 2out-of-3 voting logic. If the channel bypass is not applied to the channel experiencing a single failure, then the resulting voting logic would remain as 2-out-of-4, if the single failure does not cause a spurious trip condition. However, the resulting voting logic would become 1-out-of-3 if the single failure causes a spurious trip condition.

[Response to ‘Describe how the voting logic would be altered for reactor trip and ESF functions for the maintenance bypass mode of one channel’]

Section 7.2.1.6 of DCD Tier 2 and Section 4.2.1.6 of the Safety I&C System technical report provide the design information that a trip channel bypass results in the system performing 2-out-of-3 coincidence logic.

[Response to ‘Describe how the voting logic would be altered for reactor trip and ESF functions for a single failure of one channel and the maintenance bypass mode of another channel’]

Based on the information presented above, the resulting voting logic would become 1-out-of-2 if the single failure of one channel causes a spurious channel trip condition while another channel is placed in bypass. However, the resulting voting logic would become 2-out-of-2 if a single failure does not cause a spurious channel trip condition while another channel is placed in bypass.
Most likely, a single failure of one channel occurs in either side of the two redundant PPS cabinets within one channel. If a single failure occurs in one PPS cabinet of that channel and does not cause a spurious channel trip condition, then the resulting voting logic would remain as 2-out-of-3 while another channel is placed in bypass because the other PPS cabinet of the channel with the single failure is capable of performing its safety function.

[Response to ‘Provide design information on where the maintenance bypass mode will be set and reset for a channel’]

The terms ‘maintenance bypass’ and ‘trip channel bypass’ are identical in meaning.
The following sections of the application documents provide information regarding where the maintenance bypass mode can be set and removed.

Section 4.2.1.6 of the Safety I&C System technical report provides the following:

“Trip channel bypass is activated by a hardwired trip channel bypass switch on the MTP switch panel. Trip channel bypass switches on the MTP switch panel in the MTP/ITP cabinet (MTC) are connected to the bistable processor (BP) digital input (DI) module.”

Section 7.2.1.6 of the DCD Tier 2 provides the following:
“An individual trip channel bypass is possible on each MTP switch panel for each bistable trip. Trip channel bypass is used when removing a trip channel input from service for maintenance or testing.”

Supplemental Response

The following descriptions regarding the PPS design features will be added to Section 4.2.2.1 of the Safety I&C System technical report:

“*A trip channel bypass is applied to the channel where a single failure has occurred to avoid spurious reactor trip and ESF initiation due to that channel, resulting in a 2-out-of-3 voting logic. If the channel bypass is not applied to the channel experiencing a single failure that does not cause a spurious trip condition, then the resulting voting logic would remain as 2-out-of-4. However, the resulting voting logic would become 1-out-of-3 if the single failure causes a spurious trip condition.*

The resulting voting logic would become 1-out-of-2 if the single failure of one channel causes a spurious trip condition, while another channel is placed in bypass. However, the resulting voting logic would become 2-out-of-2 if a single failure does not cause a spurious trip condition, while another channel is placed in bypass.

A single failure of one channel normally occurs in either side of the two redundant PPS cabinets within one channel. If a single failure occurs in one PPS cabinet of that channel and does not cause a spurious trip condition, then the resulting voting logic would remain as 2-out-of-3 while another channel is placed in bypass because the other PPS cabinet of the channel with the single failure is capable of performing its safety function.”

Also, it will be indicated in Section A.6.7 of the Safety I&C System technical report that the term “maintenance bypass” is the same as “trip channel bypass.”

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Section 4.2.2.1 and A.6.7 of the Safety I&C System technical report will be revised as indicated in the attachment associated with this response.

The PPS produces discrete output signals from each channel including:

- Pre-trip and trip signals used for RPS initiation, status and alarms
- Pre-trip and trip signals for each ESFAS initiation, status and alarms

Bistable trip inputs from a BP to the LCL processors are bypassed to perform maintenance and/or testing for instrument channel inputs to permit continued operation with a bypassed channel. The trip channel bypass changes the 2-out-of-4 voting logic to 2-out-of-3 coincidence.

Monitoring, testing and maintenance of the PPS is provided using both the MTP and ITP located in each safety division.

Insert the description on the next page.

The PPS design includes the following features:

- Based on common PLC platform (see Common Qualified Platform Topical Report
- The common PLC platform provides for standardization of components, to minimize personnel training and spare parts inventory.
- Fiber optic cables and common PLC platform standard data communication are used to the extent practical.
- Software is designed, developed, tested and qualified in accordance with the SPM TeR.
- Non-combustible and heat resistant materials are used wherever practical and temperature alarms are included in the cabinet design.
- The PPS is designed and manufactured to satisfy Quality Class Q requirements and complies with the applicable codes and standards.
- The PPS is qualified to meet Class 1E and seismic Category I requirements. Class 1E is defined by IEEE Std. 603-1991 and seismic Category I is defined by RG 1.29.
- Security provisions within the PPS design include:
  - Equipment located within the PPS cabinets is administratively controlled by door key locks to protect against unauthorized access.
  - Provisions are provided by door switches to remotely indicate (via IPS/QIAS-N) that access has occurred to the PPS cabinets.
  - The PPS common platform operating system, base software and application software are protected against unauthorized alterations by a combination of cyclic redundancy checksums (CRCs) and control of access to software media.

The PPS is designed for fail safe operation under component failure or loss of electrical power.

- A single 120 volts alternating current (Vac) power is provided to redundant direct current (DC) power supplies in each PPS division. A loss of the 120 Vac power feeds to a PPS division causes the safety outputs for the division to fail to the predefined safe state.

A trip channel bypass is applied to the channel where a single failure has occurred to avoid a spurious reactor trip and ESF initiation due to that channel, resulting in a 2-out-of-3 voting logic. If the channel bypass is not applied to the channel experiencing a single failure that does not cause a spurious trip condition, then the resulting voting logic would remain as 2-out-of-4. However, the resulting voting logic would become 1-out-of-3 if the single failure causes a spurious trip condition.

The resulting voting logic would become 1-out-of-2 if the single failure of one channel causes a spurious trip condition, while another channel is placed in bypass. However, the resulting voting logic would become 2-out-of-2 if a single failure does not cause a spurious trip condition, while another channel is placed in bypass.

A single failure of one channel normally occurs in either side of the two redundant PPS cabinets within one channel. If a single failure occurs in one PPS cabinet of that channel and does not cause a spurious trip condition, then the resulting voting logic would remain as 2-out-of-3 while another channel is placed in bypass because the other PPS cabinet of the channel with the single failure is capable of performing its safety function.

EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).”

Analysis:

(i.e., trip channel bypasses)

The bypasses are always set manually as there are no automatic bypass provisions for maintenance bypasses for the PPS.

The bypass of the PPS parameters changes 2-out-of-4 logic of the PPS to 2-out-of-3 logic. The bypass of the BOP ESFAS changes 1-out-of-2 logic to 1-out-of-1 logic.

The BISI in the MCR are designed to meet the RG 1.47. The PPS channel can be placed in Manual Bypass mode to facilitate maintenance activities. Indication is provided in the main control room whenever a PPS channel has been administratively bypassed for maintenance or taken out of service.

The PPS is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. If the PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the MCR. During such operation, the PPS continues to satisfy the SFC.

The FMEA for the PPS assumes that one of the initial conditions is a PPS channel is placed in the Bypass Mode. This initial condition imposed on the FMEA determines the overall effect of an evaluated failure on the safety system’s capability to perform the required safety functions in this non-conservative mode.

The PPS supports maintenance activities, such as periodic maintenance, instrument loop testing, troubleshooting, etc. Access to features beyond displaying data such as the maintenance bypass would be under strict administrative and physical controls. These activities would be performed in accordance with site-specific administrative (procedural) and physical-access controls to set and/or change addressable constants, setpoints, and testing while the channel is in bypass mode. Such procedures would require manipulation of the FE keyswitch.

RPS and ESFAS parameters can be bypassed for maintenance. When one channel is in bypass, the coincidence logic in the LCL reverts to 2-out-of-3. The administrative procedure prohibits more than one channel from being placed in bypass.

The protection functions of the RPS and ESFAS are maintained while the system is bypassed.

A.6.8 Setpoints

Clause 6.8:

“6.8.1 The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.

6.8.2 Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.”